Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A method for generating a shared key comprising:
providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters;
performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer;
providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;
performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;
performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

[c2] The method according to claim 1 wherein the first certificate is a DSA type certificate.

[c3] The method according to claim 2 wherein the first and

second parameters comprise a prime number p_{dss}, a prime number $q_{dss,}$ a generator g_{dss} and a public key for the first and second peers, respectively.

[c4] The method according to claim 3 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss} \wedge X_R \bmod p_{dss}$ where X_R is a one-time private key from the second peer.

[c5] The method according to claim 4 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{SSK} = Y_{Adss} \wedge X_R \bmod p_{dss}$ where Y_{Adss} is a DSS public key from certificate of peer A.

[c6] The method according to claim 5 wherein $Y_{Adss} = g_{dss} \wedge X_{Adss} \bmod p_{dss}$ where X_{Adss} is a DSS private key from certificate of peer A.

[c7] The method according to claim 5 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$ where X_{Adss} is a DSS private key from certificate of peer A.

[c8] The method according to claim 1 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

[c9] An article of manufacture comprising:

a machine accessible medium including data that, when accessed by a machine, causes the machine to perform operations comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters;

performing a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer;

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;

performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

[c10] The article of manufacture according to claim 9 wherein the first certificate is a DSA type certificate.

[c11] The article of manufacture according to claim 10 wherein the first and second parameters comprise a prime number p_{dss}, a prime number q_{dss},a generator g_{dss} and a

public key for the first and second peers, respectively.

[c12] The article of manufacture according to claim 11 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss} \wedge X_R \bmod p_{dss}$ where X_R is a one-time private key from the second peer.

[c13] The article of manufacture according to claim 12 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{SSK} = Y_{Adss} \wedge X_R \bmod p_{dss}$ where Y_{Adss} is a DSS public key from certificate of peer A.

[c14] The article of manufacture according to claim 13 wherein $Y_{Adss} = g_{dss} \wedge X_{Adss} \bmod p_{dss}$ where X_{Adss} is a DSS private key from certificate of peer A.

[c15] The article of manufacture according to claim 13 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$ where X_{Adss} is a DSS private key from certificate of peer A.

[c16] The article of manufacture according to claim 9 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

[c17] A system comprising:

a processor; and

a memory coupled to the processor, the memory containing program code that, when executed by the processor, causes the processor to:

provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters;

perform a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer;

provide a second certificate and the first public key from the second peer to the first peer; the second certificate comprising a plurality of second parameters;

perform a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

[c18] The system according to claim 17 wherein the first certificate is a DSA type certificate.

[c19] The system according to claim 18 wherein the first and second parameters comprise a prime number p_{dss}, a

prime number q_{dss}, a generator g_{dss} and a public key for the first and second peers, respectively.

[c20] The system according to claim 19 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss} \wedge X_R \bmod p_{dss}$ where X_R is a one-time private key from the second peer.

[c21] The system according to claim 20 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{SSK} = Y_{Adss} \wedge X_R \bmod p_{dss}$ where Y_{Adss} is a DSS public key from certificate of peer A.

[c22] The system according to claim 21 wherein $Y_{Adss} = g_{dss} \wedge X_{Adss}$ where X_{Adss} is a DSS private key from certificate of peer A.

[c23] The system according to claim 21 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$ where X_{Adss} is a DSS private key from certificate of peer A.

[c24] The system according to claim 17 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

[c25] A method comprising:

receiving a first certificate including a plurality first pa-

rameters;

performing a first exponentiation operation to generate a first public key using at least one parameter of the plurality of first parameters and a first private key;

receiving a second certificate and the first public key, the second certificate including a plurality of second parameters;

performing a second exponentiation operation to generate a first shared secret key using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate a second shared secret key using the first public key and a private key.

[c26] The method according to claim 25 wherein the first certificate is a DSA type certificate.

[c27] The method according to claim 26 wherein the first and second parameters each comprises a prime number p_{dss}, a prime number q_{dss},a generator g_{dss} and a public key.

[c28] The method according to claim 27 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss} \wedge X_R \bmod p_{dss}$ where X_R is a one-time private key.

[c29] The method according to claim 28 wherein the second

exponentiation operation to generate the first shared secret key for the second peer is $Y_{SSK} = Y_{Adss}\text{^}X_R \bmod p_{dss}$ where Y_{Adss} is a DSS public key.

[c30] The method according to claim 29 wherein $Y_{Adss} = g_{dss}\text{^} X_{Adss} \bmod p_{dss}$ where X_{Adss} is a DSS private key.

[c31] The method according to claim 29 wherein the third exponentiation operation to generate a second shared secret key is $Y_{SSK} = Y_R \text{^} X_{Adss} \bmod p_{dss}$ where X_{Adss} is a DSS private key.

[c32] The method according to claim 25 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.